Cybersecurity Economics: Induced Risks, Latent Costs, and Possible Controls

ED Frangopoulos, MM Eloff, and LM Venter

Abstract: Financial decisions indirectly affect and are affected by the effort towards Information Security. The 'Economics of Cybersecurity' should thus constitute a significant part of the Information Security Posture Assessment process and should be directly addressed in this context. As the complexity and interdependency of Information Systems augments and new technologies lead to the de-materialization of Information Systems assets, it becomes progressively evident that the conflicting interests and incentives of the various stakeholders of an Information System affect its overall Information Security Posture, perhaps even more significantly than technical or policy limitations do. This paper examines economic considerations from an Information Systems Security/Cybersecurity viewpoint and proposes new directions that may both help reduce the problem from a collective point of view, as well as lead to the creation of methodologies to ultimately integrate economics, along with technical and non-technical issues, into an Organisation's Information Security Posture Assessment process.

Keywords: *Cybersecurity, Economic Considerations, Risk Management, Infosec Economy, Cybersecurity Controls, Cybersecurity Costs*

Introduction

It is a generally accepted truth that Information Security (IS) costs money. There are inherent costs in all aspects involved in the mitigation of the risks relevant to IS, such as the technology used, required procedures, statutory compliance, awareness education, etc. The same holds true for Information System Security, or Cybersecurity, which is the IS subset that deals with Information Systems aspects of IS (what used to be known as 'computer security'). The expenditure for IS has been steadily increasing over the past years, following the increase in emerging Cybersecurity threats as it has been established in the recently released 'The Global State of Information Security® Survey for 2014' (PwC 2013b). The 'Emerging Threats' versus 'Cybersecurity initiatives' race is being viewed as the modern cold war face-off, which is constantly fuelled by large numbers of emerging threats as categorically shown in the ENISA Threat Landscape 2013 report (ENISA 2013). Unfortunately, it may well be that even though IS expenditure increases, it does not do so at a rate capable of efficiently counteracting the emerging threats. Furthermore, the attackers are no longer lone hackers driven by personal agendas, but there may well be criminal organisations or even nations behind cyber- offensives.

The ugly truth is that this 'war' is definitely asymmetric, as the attackers have many weapons in their arsenal and attacks can be mounted with low cost, compared to the possible gain stemming from a successful attack. On the contrary, regarding the defensive side, any 'Cybersecurity initiative' faces the real risk of becoming a bottomless money-pit or, if funding is prematurely curtailed, of not being able to justify its existence, and, even worse, of potentially providing a false sense of security to the defending force. In the preface to their book titled 'Foundations of Information Security: Based on ISO27001 & ISO27002', Hintzbergen *et al.* (2010) make reference to the Great Wall of China as the ultimate example of the effort towards physical security and the effect of physical security in modern-day IS. The Great Wall of China, and fortress walls in general, are indeed very popular examples used in the IS literature (Groom 2003) from which analogies are drawn (for example, Bastion hosts and Gateway servers). However, the Great Wall of China can also be used to

demonstrate the asymmetry of cyberwar. The Great Wall was built at great expense and effort, yet it too had vulnerable points, partly due to terrain and partly due to the limitations in its construction. A single well-targeted attack against the wall could result in a breach, and thus the cost of intrusion would be negligible compared to the total cost of construction and maintenance of the Great Wall.

It is thus not unfitting to draw analogies from this example for the Cybersecurity paradigm, whereby the equivalent 'Great Wall' is constructed of a plethora of technical measures, supported by policies and procedures. The problem, though, frequently lies in the 'brick and mortar' of this construct and manifests itself in the form of hastily produced and inadequately debugged software that, when integrated in the wall-building effort, comes with inherent defects and weaknesses. This is usually caused by the desire of software houses to minimise the time-to-market of a new product and to maximise the profit on the relevant investment. Other problems with the 'construction material' of the 'wall' may result from choices made by the defending champions regarding the selection and integration of security-crucial components which are, once more, influenced by financial considerations. Furthermore, insofar as policies and procedures are concerned, they, too, are governed by direct financial decisions as well as by indirect ones, such as those that are related to productivity, financial risk, reputation issues, etc. Hence, financial decisions made within the boundaries of an organisation increasingly affect its vulnerability horizon.

Vulnerabilities Induced by Economic Considerations

Economic considerations are being used in the process of risk assessment, usually to define an organisation's 'risk appetite' and to lead to informed decisions regarding the implementation of security measures. Even though there is nothing intrinsically wrong with this procedure, which does indeed produce valid results, perhaps a change of paradigm is in order: the economic considerations themselves should form part of the threat landscape that needs to be examined in the context of a risk assessment. In such an approach, economic considerations will not only function as the yardstick against which every type of risk and its compensatory measures are benchmarked, but they, too, will come under scrutiny and evaluation. In the following sections, an effort is made to bring to light a number of economic considerations that give rise to vulnerabilities or may even be themselves identified as vulnerabilities for IS. The question that needs to be addressed is whether and to what extent the economic considerations that may seem justified from the Management's point-of-view adversely affect IS, and Cybersecurity in particular, and if these can be somehow controlled.

Diverging incentives and holes-in-the-wall

It was already mentioned that the defensive wall that organisations are trying to build around their information assets may be undermined by the different incentives of the organisation and of the software and hardware vendors. One such difference may indeed be the fact that software vendors are commonly more concerned with the production of buyer-acceptable software at minimum cost and with minimal time-to-market, rather than with the effort towards the security of their product (Anderson & Moore 2006) which is usually exhausted at the lowest obligatory level prescribed by regulatory compliance (Shostack & Stewart 2008). It is interesting that, in this day and age, software houses still shy away from assuming any of the risk stemming from the use of their products (Marotta-Wurgler 2007 & 2011). In order to use the software, clients have to accept disclaimers that minimise or even eliminate the liability of the software producer/vendor. Effectively, as Bessey *et al.* (2010) put it: "Indifference can arise from lack of accountability".

However, even though users may like the idea of secure software, they can neither really tell the difference between secure and insecure software nor are they inclined to pay for better- written software. Thus, because of competition, the costly effort that goes into the production of secure software cannot be adequately compensated for (Anderson & Moore 2006). This, in turn, makes it difficult for software houses to allocate funding and resources for the production of secure software. If software security were somehow enforced (for example through legal/regulatory compliance to appropriate standards and practices), software would probably cost significantly more than it does today. The problem of diverging incentives between the software houses and their ultimate clients becomes even more serious if stories, such as the one reported by Reuters (2013) exposing a secret $10 million contract between RSA and NSA, prove to be true. If products by Information Security giants that are used by hundreds of software producers and service providers are tainted in the manner reported by Reuters, then innumerable end-users ranging from individuals to corporate and governmental entities and to international organisations, are adversely and grossly affected.

Upgrading towards greater risk

The function of Information Systems in a constantly changing landscape of emerging threats requires systematic updates in order to maintain an acceptable level of Cybersecurity. Continuous updating is in part necessitated by initial inadequate debugging of software code. Hence, updates become tools for fixing bugs

and addressing security liabilities during the production phase of software (Brown 2005). Complete debugging becomes virtually impossible given the complexity of the code and the constraints imposed on software production by economic considerations. It is also assumed that once a 'patch' is applied in order to control an existing shortcoming in the code or to provide new functionality, the additional code may itself have new and different shortcomings that create new vulnerabilities to be addressed and so on. However, it is reasonable to assume that with every iteration of the update process, the software tends asymptotically to a state of higher security that should eventually -- *ceteris paribus* -- lead to a higher level of Cybersecurity. Unfortunately, all other things do not remain constant, and 'new and improved' versions of the software, inescapably give rise to a myriad of new vulnerabilities.

In practice, even if not required or requested by the customer, the upgrade to the new version of the software is compulsory--usually at significant cost--as support for previous versions is discontinued eventually and thus they become obsolete. The new versions, in order to provide increased functionality that appeals to the customer, are always more complex, and have more lines of code and thus include more bugs, effectively feeding the vicious cycle of the continual struggle towards Cybersecurity. The paradox of this situation is that the end-user invariably uses only a small fraction of the software's full functionality. By trying to address the differing individual needs of their clientele all at once, the software producers create coding behemoths that are impossible to contain from a security perspective. The end result is that the customers are forced to accept increasingly expensive and at the same time more vulnerable software that requires a larger number of more expensive controls. Hence, software becomes more expensive and less secure.

Who decides on what matters

At the foundation of every Risk Assessment project lies the valuation of assets. This is necessary in order to establish controls that are commensurate with the asset value. Asset valuation is rarely a simple task and it becomes increasingly complicated given the pervasive nature of Information Technology and the maze of interdependencies between business functions and assets. In an organisational structure, the obligation for an authoritative opinion on information asset valuation lies with the business owners of the information assets, although it is usually the Information Technology department which is responsible for the actual security of the assets. Clearly, the views that the two groups take on the same assets are from radically different perspectives and, hence, the resulting opinions and argument lines are usually quite different. In a context of cutbacks and limited resources, 'efficient' governance may call for a 'relaxed' view on the value of a particular asset to the business, with the ultimate goal of keeping the relevant security budget in check. Such an attitude may cause serious problems in the function of the IT department that will simply not have the means to adequately care for the security of the information assets it is entrusted with. Thus, an organisational strategy which only looks at the 'bottom-line' may create latent security issues that will eventually undermine the Information Security structure as a whole, due to the interdependencies between information assets and business functions. Better communication between the different groups within an organisation may help in the direction of more accurate asset valuation, but, again, this may prove to be ineffective as it is commonplace for executives in general and Information Security executives in particular to be required 'to do more with less' (Johnson & Goetz 2007).

In a business context of limited financial resources, the pressure on employees of all levels to perform beyond

what can be reasonably expected from them serves as a negative influence on their acts and decisions, especially those related to Information Security which is usually viewed in an oversimplified manner. Research carried out by Albrechtsen and Hovden (2009) further shows that different groups within an information-handling structure perceive matters differently, thus leading to misconceptions about Information Security and to a lack of common understanding of Information Security and Information Assurance concepts. Furthermore, in the context of austerity, the ever-present problems in communication and understanding between groups of stakeholders of the same organisational structure, as identified by Berger and Luckmann (1991), become more prominent, in effect leading to a breakdown of communications between the different groups of stakeholders. Thus the lack of common understanding between Information Security managers and everyone else in the Organisation (possibly including those responsible for information asset valuation) combined with the aggravated difficulties of communication between groups, makes it difficult to accurately set the true value of information assets to the organisation.

To complicate the issue even further, as the attack vectors against information resources continually evolve and become more elaborate, perhaps it is the exploitation value that an information asset potentially holds for an attacker that must be examined, along with its obvious business value. If, for example, the comparative values of an organisation's customer database versus its employee database are examined (the sensitive personal data protection regulatory compliance notwithstanding), from a business point of view it is the customer database which is more important and thus warrants stricter (and more expensive) protective measures. Hence, a higher budget will be allocated for the security of the customer database rather than for the employee database. From the attacker's side though, the employee database may be very attractive and may have a very high exploitation value as a means to successful attacks against other assets of the organisation. Viewed from that angle, a high security budget may also be justified for the protection of the seemingly business-wise inconsequential employee database.

Productivity versus Security

Information Systems Security/Cybersecurity measures are often seen as inhibitors of productivity. This may manifest itself at the user level where, for example, USB port deactivation or the necessity for many and complex passwords may cost time and effort on the part of the user. Hence, the user may feel that this is a waste of resources that reduces his or her productivity and eventually the profits of the business. When this view is shared by the management (after all, managers are usually also users of the same Information System), then:

a) at a critical time management might directly or indirectly force the users or even IT administrators to break away from the Information Security Policy (ISP) and circumvent the controls in order 'to get the work done' (the image of a CEO wielding a tablet and asking IT people to connect it to the network despite ISP provisions, does spring to mind), or

b) management might oppose the inclusion of controls that might feel counter-productive and thus financially unwise-- in the ISP, effectively undermining the Cybersecurity effort. This is corroborated by the findings of Rainer *et al.* (2007) where the list of top issues that Information Security professionals have difficulty addressing with management includes 'top management support', 'low funding', and 'justifying security expenditures'.

Moving away from the 'Moat & Castle' cybersecurity model

Pfleeger (1997) used a medieval analogy of a castle surrounded by a moat in order to explain the idea of 'defence-in-depth' in Information System Security. This has been and still is the model through which most information assets are protected. However, in the interest of enhanced productivity, which directly translates to profit maximisation, business management continually requests greater availability of information assets, irrespective of the geographic location of users and time-of-day. From low-end IT users to business managers, we are all enticed by the flexibility and mobility that technological solutions provide for our everyday lives and we are willing to sacrifice large parts of our privacy and right to confidentiality in order to keep enjoying this maximised availability of information. Being accepted at a personal level, this model is then unreservedly requested for the management of professional information by turning a blind eye to the extended security requirements that apply to this type of information. In order to provide such services and to facilitate relatively new and 'financially sensible' notions such as 'Bring Your Own Device' (BYOD) and the use of the Cloud, Information Systems have to move away from the Pfleeger 'Moat & Castle' paradigm and, in the attempt to remain secure, confront a huge set of new threats. It could be argued that this is evolution and progress and that it should not be hindered but, instead, adaptation is in order. However, recent history has shown that the move towards new technologies is anything but systematic and controlled as far as the security of these new technological solutions is concerned (GIT 2013). On the contrary, technical solutions are proposed and adopted on short-term and immediately visible economic merits--or the expectation thereof before the degree of their security resilience is even established, which can lead to great loss, financial and otherwise, during their maturation. Typically, even though we are being taught that security considerations for a proposed solution should begin at the time of its conception, the fact remains that most of the IT industry generally works under the principle of putting a new product out for sale as quickly as possible and worrying about its security parameters later. Thus, we find ourselves stepping outside the relatively secure perimeter defined by the 'Moat & Castle' in order to gather larger crops, without having first ensured that we have a fighting chance against an enemy attack.

Outsourcing and expansion: can Information Security levels be sustained?

In current times of globalisation and a continual search for the competitive edge, business choices often call for outsourcing of information-related services to third parties and expansion of the business on its own means or through partnerships. Such business choices are usually made without prior investigation of the new security risks that they may be causing (Johnson & Goetz 2007). To use the Great Wall of China example, in time of rapid territorial expansion, the frontier line quickly grows in length, without a strong wall to protect it against attacks. Defending that line is probably the most difficult task following an expansive campaign. Hence, for businesses, the challenge is to follow the prescribed business plan, without losing control of the information assets of the business and without compromising the assets' security. Additionally, the challenge becomes even greater when expansion includes acquisitions or makes systems accessible by external partners (Johnson & Goetz 2007). When outsourcing information-related services to third parties, the utmost care must be taken, as third-party organisational structures are not necessarily permeated by the same Cybersecurity mentality of the outsourcing organisation, and they might not share the same values. Auditing or random checks of the third-party procedures and practices by the outsourcer are usually out of

the question, so the cooperation between the two parties is simply governed by an agreement which addresses Information Security issues as a subset of a more general context and even prescribes penalties in case of non-compliance. If the common Cybersecurity effort is exhausted at that level, it is quite possible that trouble will not be avoided and all action will be retroactive, following a security event. Following a common rule, such as the one set by the ISO/IEC 27000 series standards, thus becomes of paramount importance for cooperation. This common alignment must be promoted both by the appropriate legal and regulatory framework as well as by generally acceptable best business practices.

To be or not to be (secure)?

In the various certification programs for Information Security professionals (as in ISACA 2011) it is taught that the effort towards Information Security should function as a business enabler by a) being aligned with business goals and objectives, b) ensuring regulatory compliance, and c) reducing risk to an acceptable level. These are valid working hypotheses, as, indeed, overspending on Information Security would be unwise and would have adverse effects on the 'bottom line' of the business. In this sense, several spending models and investment approaches for Information Security have been developed (as in Gordon & Loeb 2002; Cavusoglu, Mishra & Raghunathan 2004; Tsiakis & Stephanides 2005; Böhme 2010, etc). It is beyond the scope of this paper to compare and to analyse Information Security spending models and a very extensive bibliography exists on the subject. However, despite the outcome of a model-based expenditure analysis--with all of its merits and shortcomings-- the ultimate business decision on information security must be aligned with the core business objective and it must be made by people whose roles are closer to management than to Information Security. Schroeder and Grimaila (2006) showed that there is definite bias in the decision-making process regarding Information Security and that the decision-makers "will place more weight on operational outcomes than security outcomes". Thus, even if security considerations are against the operation of a system, the decision-makers are perfectly capable of ignoring that outcome, simply because the business impact of not having the system in operation is greater than allowing it to function without sufficient security. If such economics- based decisions are abused, they will significantly raise the organisation's risk appetite and undermine its Cybersecurity posture.

Regulatory provisions as an excuse

Apart from business alignment and acceptable risk, as examined above, there is also the issue of regulatory compliance. It is evident that defensive action in Cybersecurity always comes as a result of an exploited vulnerability. Strictly speaking, pro-active cyberdefence--in the exact meaning of the term--is not really possible. Most cyberdefence measures are thus one step behind the respective threats in this continual tug-o-war. To make matters worse, for such a measure to be included in a regulatory compliance document, even more time has to pass. It is thus only reasonable to conclude that regulatory provisions only cater for 'yesterday's problems'. This is no secret among serious Information Security professionals, and thus regulatory compliance is, by default, considered inadequate in real Information Security and Cybersecurity terms. On the other hand, regulatory compliance gives a golden excuse to Management to limit Information Security expenditure because it simply allows the tick-off of another checkbox in a financially justified 'to do' list, without effectively addressing the underlying security issue (Shostack & Stewart 2008).

A cloudy future

While the move towards the cloud does seem to have some obvious financial advantages, the cloud still remains a very unsafe place for storing information (GIT 2013). Furthermore it constitutes an example of how large IT vendors use their market penetration to further shape the market (and its security) according to their interests. The degree of success of a Cloud service provider depends on the provider's ability to create service capacity at a much larger scale than any individual organisation could manage and then sell it back to the user piecewise at a gain, but at a much lower cost than the user could manage alone (Kushida, Murray, & Zysman 2011). In order to attract customers quickly, the major cloud service providers created a very attractive but quite unsafe environment. According to the Georgia Institute of Technology "Emerging cyber threats report 2014" (GIT 2013), for data to be moved to the cloud there must be trade-offs between security and usability as "File sharing and other cloud services still have questionable security". The report identifies three key issues that, despite all predictions to the contrary, persist: a) business data is moved to the cloud protected only by the security measures provided by the cloud storage firm, b) private- key encryption is not used, as storing encrypted data in the cloud drastically reduces the cloud's utility, and c) the use of searchable encryption necessitates trade-offs between security, functionality, and efficiency. Yet, even though security is all but non-existent in the cloud, companies and organisations exhibit a huge appetite for risk by deciding to keep using it, obviously basing their decision on financial merits alone. Even hardware methods of controlling who has access to cloud data and where data is stored, through the use of Trusted Platform Modules or 'TPM' as described by Krauss and Fusenig (2013), may be insufficient, as even these most secure Integrated Circuits (ICs) have been reported to succumb to physical attacks using acid, rust remover, a lot of time, and a lot of skill (Tarnovsky 2008). As TPM ICs are used in many sensitive applications such as secure communications, military systems, and the like, it is conceivable that if enough money and resources are allocated to the effort, a great deal of secrets can be had; once again, this is an economic dilemma.

Cutting chip corners

Since the 1980s, the hunt for lower production cost and profit margin maximisation on digital equipment has led to a shift of Integrated Circuit foundries, from their birthplace in Silicon Valley to the Far East (Perera 2012). This has resulted in most of the big names in IC design becoming 'fabless' producers (as producers without fabrication facilities of their own are called) who subcontract the production of their designs to independent foundries, mostly in the Far East. According to the Solid State Technology Insights website (SST 2012), foundries in Taiwan, South Korea, and China occupied 9 of the 12 top worldwide spots of semiconductor foundries for 2012. (The US is still present on the list with two foundries and Israel with one.) For China, in particular, according to PwC's report on "China's impact on the semiconductor industry 2013 update" published in September 2013 (PwC 2013a), China's semiconductor consumption market grew by 8.7% in 2012 to reach a new record of 52.5% of the global market, while its share of worldwide electronic equipment production increased to 34.2% in 2012 and is expected to increase to more than 40% by 2017. Accordingly, China's share of worldwide semiconductor production reached 12% in 2012 and is expected to reach at least 14% by 2015. The reliance of the world electronics industry on far-eastern semiconductors, a choice made on the grounds of lowering the cost of production, appears to have a darker side: for many years there have been rumours that Integrated Circuits may contain 'undocumented features' ranging from 'kill switches' to backdoors. One of the first sensational stories about a kill switch had to do with the temporary 'blindness' of Syrian radars when Israeli bombers carried

out a raid in 2007 against Syrian targets (Adee 2008). Compromised ICs in the radar systems, containing a 'kill switch', were blamed at the time and theories about creating hardware backdoors on ICs followed. Recently, Skorobogatov and Woods (2012) provided an end to the rumours by actually locating a backdoor on a military microchip fabricated by an independent foundry for a fabless IC producer.

Given the proliferation of personal mobile devices and the evolution of 'Internet of Things' which is already well under way, the implications of the use of ICs with malicious payload on Cybersecurity are obvious. The risk increases as tools like the 'Shodan' engine (www.shodanhq.com) which searches for exposed devices on the Internet, are becoming available. Unless procedures for secure and authenticated manufacture of ICs as well as methods for full post-production verification of ICs are devised (something which at this point proves to be very difficult), hundreds of millions of individuals, corporations, and organisations around the world will face unprecedented risks. However, the cost for the required procedures and methods will be significant and it remains to be seen if the producers of equipment will decide to accept the cost or prefer the creation of new vulnerabilities for the sake of the 'bottom line'.

Proposed Controls

The presented cases only serve as examples of how considerations of an economic nature may directly or indirectly introduce vulnerabilities that undermine the effort towards Cybersecurity. One of the obvious questions is, thus, whether effective controls can be devised. Such controls should both address the risk which is linked to the general environment of the current IT market that is beyond the control of any single organisation as well as the risk which is induced by decisions made within an organisation's boundaries.As far as bad coding is concerned, this could be addressed through compulsory compliance with improved software industry standards that enforce secure coding practices such as the ones presented by CERT (2011) and OWASP (2010). As the infrastructure for assessing the structural quality of software and non-functional requirements, based on code metrics, does exist (e.g. standards ISO/IEC 25010:2011 [ISO 2011] and 9126-1:2001 [ISO 2001]), it is only a matter of creating mechanisms that ensure code compliance to secure coding standards or to improve existing ones (Devanbu & Stubblebine 2000; Chen & Wagner 2002; Baggen, Schill, & Visser 2012). A widely-recognised seal of approval could then be given to security- compliant software.

For this idea to bear fruit, it will be necessary for major software houses to be convinced to support it based on its long-term merits for the market, rather than to oppose it because of the short-term financial burden that it might cause. Such a change in mentality could be assisted by a regulatory framework that rewards secure coding practices and inflicts penalties for the lack thereof.A change of mentality might also be in order insofar as users' expectations from software are concerned. Instead of using complex and thus security-challenged software, a decision should be made to use simpler software without superfluous functionality but with fewer security deficiencies. Software should be tuned to an organisation's needs following an accurate requirements' analysis. This will not lead to cheaper software but it will help allocate funding more prudently towards increased and distributed Cybersecurity. Modular programming could help towards this end, as presented, amongst others, by Chen & Wagner (2002), Bauer, Appel, & Felten (2003), and Dhiman *et al*. (2013).

To aid in this direction, markets for vulnerabilities (created by companies that purchase zero- day information on

vulnerabilities and then re-sell it exclusively to their clients for a profit), can be used to quantify software security, thereby rewarding good programming practices and punishing bad ones as proposed by Anderson & Moore (2006).In the above context, if insurance against cyberattacks matures, it will be helpful, through the provision of metrics, for quantifying risks induced by poorly-coded and security-challenged software. Additionally, accurate evaluation of the cyber-risk levels of organisations will act as an incentive towards better Cybersecurity. Organisations will be keener to adopt cyberdefence practices as this will reduce their Cybersecurity insurance premiums, leading to a distribution and normalisation of the Cybersecurity effort in a manner similar to which vaccinations help eradicate diseases: they work only if, ideally, everybody participates. Stricter regulatory compliance should be in place so that when software houses, service providers, or infrastructure producers are found to have been negligent concerning the protection of the interests of their customers/end-users, or, worse, if they have been knowingly working against these interests, the loss suffered by the users should be transferred in part or in whole to the offending party. Given the de-materialisation of Information Systems assets, this can only be made possible through the application of international law.

In order for correct business choices to be made by taking Cybersecurity issues into consideration during business expansion and/or information-related task outsourcing, the following conditions must be met: a) Top-level Management must work closely with Information Security/Cybersecurity executives and must heed their advice in the decision- making process; b) Top-level Management must actively engage in and support the creation of a Cybersecurity culture. They should also lead by example and should promote Cybersecurity as a core component of the business; c) Information Security/Cybersecurity executives must be involved in and have a solid understanding of the business objectives. This is the only way that their expertise can be used efficiently for enabling the business. Technical skill alone is not sufficient, and; d) Homogeneous Cybersecurity must be applied across the Organisation and its partners in order to avoid weaknesses or 'holes-in-the-wall'.As far as cloud technologies are concerned, their further development must include effective Information Security and Assurance controls by design. Experience shows that security that comes as an afterthought which is then 'bolted-on' to an existing product or service, only becomes effective at great difficulty and expense, compared to security being incorporated into the product's or service's design from its earlier phases. As cloud services do suffer from such a predicament (GIT 2013), a good step towards the normalisation of cloud service security is expected to be made by the publication of the announced addition to the ISO/IEC 27000 series of standards. The ISO/IEC 27017 standard which is currently under development with an anticipated date of publication towards the end of October 2015 (ISO 2014a), is expected to provide the necessary framework for cloud service security in line with the ISO/IEC 27002:2013 (ISO 2013). Once again, even if this is not covered in ISO/IEC 27017, an appropriate international legal framework will be necessary in resolving and regulating many of the security challenges that cloud services currently face.

In order to obtain accurate information on asset valuation which in turn will be used for the proper allocation of the information security budget, close cooperation between the business owners of assets, the Information Technology actors, and the Information Security and Assurance executives is essential. Recent developments, such as the publication of the ISO/IEC standard 27016:2014 (ISO 2014), which deals in part with the organisational economics of Information Security, will eventually provide a rule against which business practices can be assessed and improved. Still, if the ISO/IEC 27016:2014 standard is seen merely as a regulatory

obligation to conform with, its value will be diminished.Finally, the gravity of the Cybersecurity component in the decision-making business process should be stressed. Information Security/Cybersecurity experts cannot be management experts and vice-versa. For this reason, security steering committees should be made up of experts from all disciplines and Cybersecurity issues should be assigned the importance they deserve and should even be given priority over 'bottom-line' financial considerations. To accomplish this, awareness programs must be more frequent and their effects be should be monitored. From the authors' experience, once decision-makers internalise the true gravity of Cybersecurity issues, they tend to heed the advice of Information Security experts more closely.

Inclusion of Information Security Economics in the Plan-Do-Check-Act (PDCA) Cycle

Regardless of the effect that controls, based on the suggestions presented in the previous section, may have, any organisation should be able to assess at any point in time its own security posture with respect to the vulnerabilities stemming -- directly or indirectly -- from financial decisions made within its own boundaries. In order to achieve this, the organisation's Information Security Management System (ISMS) will have to be adjusted to include such financially-induced vulnerabilities in the scope of the PDCA virtuous cycle. The obvious prerequisite for doing so is to identify appropriate indicators that will support the assessment process. These indicators do not necessarily have to provide discrete numeric values for the assessment process from the first iteration of the process, but should at least a) help identify problem areas in Information Security Management that warrant immediate attention, and b) provide a baseline for future iterations in order to monitor progress in the areas of concern. The results of iterations following the ones used for defining a baseline can be fed to an “Information Security dashboard” that will provide a quick an accurate picture of the current state, allowing for iterative steps of adjustment and improvement, as well as possibly highlighting emerging problem areas (Frangopoulos, Eloff, & Venter 2014).

Such indicators could include: a) the perceived level of communication between Information Security/Cybersecurity executives and Management (as viewed from both sides), b) the pervasiveness of new and possibly security-wise immature technologies in business processes, c) the gravity of Information Security/Cybersecurity considerations against financial ones in the business decision-making process (as perceived by both the Information Security/ Cybersecurity and Management groups), d) the level of adherence to legacy Information Technology projects and solutions that do not have properly built-in security controls, e) the level of involvement of Information Security/Cybersecurity executives in the business decision-making process (as perceived from both the Information Security/Cybersecurity executives and Management), and f) the level of business and information handling processes conformity to Information Security standards.The above list of indicators is definitely not exhaustive. As it is generally true for proper indicator selection, this list must be augmented and adapted to the specific needs of each organisation, always bearing in mind the goal of this exercise, which is none other than to look behind the obvious for Information Security/Cybersecurity vulnerabilities, directly or indirectly induced by considerations of a primarily economic nature.

Conclusions and Further Work

A non-exhaustive list of representative examples of economic considerations that lead to IS vulnerabilities has been examined. Controls for vulnerabilities directly or indirectly caused by economic considerations are of a financial nature themselves and where that is not effective, institutional compliance must come into play. New technologies should be allowed to mature and pass through the crucible of time before being used in IS-critical situations. Technologies used for inconsequential communication and data management should not be ported to an IS- critical environment. Software houses may have to be institutionally forced to be more honest in their marketing habits and their customers must learn to exercise self-restraint and not to be gluttonous in their IT-related desires. Users and, most importantly, decision-makers must be re-educated on the value of privacy and security in cyberspace and the collective awareness level on IS and Cybersecurity must be raised. By systematically introducing economic considerations as vulnerability inducers in the Information Security/Cybersecurity posture assessment process, an 'Information Security dashboard' for financially-induced vulnerabilities can be created. For such a monitoring system to be effective, appropriate indicators must be identified and used.

References

Adee, S 2008 'The hunt for the kill switch', *IEEE Spectrum*, vol. 45, no. 5, pp.34-39.

Albrechtsen, E & Hovden, J 2009 'The information security digital divide between information security managers and users', *Computers & Security*, vol. 28, no. 6, pp. 476–490.

Anderson, R & Moore, T 2006 'The Economics of Information Security', *Science*, vol. 314, pp. 610-613.

Baggen, R, Schill, K & Visser, J 2012 'Standardized code quality benchmarking for improving software maintainability', *Software Quality Journal*, vol. 20, no. 2, pp. 287–307.

Bauer, L, Appel, AW & Felten, EW 2003 'Mechanisms for secure modular programming in Java', *Software: Practice and Experience*, vol. 33, pp. 461–480.

Berger, PL & Luckman, T 1991. *The social construction of reality. A treatise in the sociology of knowledge*. Penguin Books, London.

Bessey, A, Block, K, Chelf, B, Chou, A, Fulton, B, Hallem, S, Henri-Gros, C, Kamsky, A, McPeak, S & Engler, D 2010 'A few billion lines of code later: using static analysis to find bugs in the real world', *Communications of the ACM*, vol. 53, no. 2, pp. 66–75.

Böhme, R 2010 'Security metrics and security investment models', *Advances in Information and Computer Security*. Springer, Heidelberg, pp. 10–24.

Brown, DJ 2005 'An update on software updates', *Queue*, vol. 3, no. 2, pp. 10–11. Cavusoglu, H, Mishra, B & Raghunathan, S 2004 'A model for evaluating IT security investments', *Communications of the ACM*, vol. 47, no. 7, pp. 87–92.

CERT 2011, *CERT Top 10 Secure Coding Practices*, viewed 18 Jan. 2014, <https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Pra ctices>.

Chen, H. & Wagner, D 2002 '*MOPS:* An infrastructure for examining security properties of software', *Proceedings of the 9th ACM conference on Computer and communications security*, ed. V Atluri, pp. 235-244.

Devanbu, PT & Stubblebine, S 2000 'Software engineering for security: a roadmap', *Proceedings of the Conference on The Future of Software Engineering*, ed. A Finkelstein, pp. 227-239.

Dhiman, K, Mai, M, Soni, J, Lam, L & Han, SA 2013 'Clojure: modular programming with functional, concurrent language on the JVM', *Proceedings of the 2013 Conference of the Center for Advanced Studies on Collaborative Research*, pp. 370-371.

ENISA 2013, *ENISA Threat landscape 2013*, viewed 1 Feb. 2014, <http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa- threat-landscape-2013-overview-of-current-and-emerging-cyber- threats/at_download /fullReport>.

Frangopoulos, ED, Eloff, MM,& Venter, LM 2014 'Human aspects of information assurance: A questionnaire-based quantitative approach to assessment', *Proceedings of the 8th International Symposium on Human Aspects of Information Security & Assurance*, eds. N Clarke & S Furnell, pp. 217-229.

GIT 2013, *Georgia Institute of Technology: Emerging cyber threats report 2014*, viewed 13 Jan. 2014, <http://www.gtcybersecuritysummit.com/2014Report.pdf>.

Gordon, LA & Loeb, MP 2002 'The economics of information security investment', *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457.
Groom, PD 2003 'The IT security model', *Potentials*, IEEE, vol. 22, no. 4, pp.6-8. Hintzbergen, J, Hintzbergen, K, Smulders, A, & Baars, H 2010. *Foundations of information security: Based on ISO27001 & ISO27002.* Van Haren Publishing, Zaltbommel.

ISACA 2011. *CISM® review questions, answers and explanations manual 2012*. ISACA, Rolling Meadows, IL.

ISO 2001, *ISO/IEC 9126-1:2001 Software engineering - product quality - Part 1: Quality model.* ISO, Geneva.

2011, *ISO/IEC 25010:2011 Systems and software engineering - systems and software quality requirements and evaluation (SQuaRE) - system and software quality models*. ISO, Geneva.

2013, *ISO/IEC TR 27002:2013 Information technology -- security techniques -- code of practice for information security controls*, ISO, Geneva.

2014, *ISO/IEC TR 27016:2014 Information technology - security techniques -information security management — organizational economics*, ISO, Geneva.

2014a, *ISO/IEC CD 27017 Information technology - security techniques - code of practice for information security controls for cloud computing services based on ISO/IEC 27002*, viewed 8 Sept. 2014, <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757>.

Johnson, EM & Goetz, E 2007 'Embedding information security into the organization', *IEEE Security & Privacy*, vol. 5, no. 3, pp. 16–24.

Krauss, C & Fusenig, V 2013 'Using trusted platform modules for location assurance in cloud networking, *Network and System Security*. Springer, Heidelberg, pp. 109–121.

Kushida, KE, Murray, J, & Zysman, J 2011 'Diffusing the cloud: Cloud computing and implications for public policy', *Journal of Industry, Competition and Trade*, vol. 11, no. 3, pp. 209–237.

Marotta-Wurgler, F 2007 'What's in a standard form contract? An empirical analysis of software license agreements, *Journal of Empirical Legal Studies*, vol. 4, no. 4, pp. 677–713.

2011 'Some realities of online contracting', *Supreme Court Economic Review*, vol. 19, no. 1, pp. 11–23.

OWASP 2010, *OWASP Secure Coding Practices Quick Reference Guide*, viewed 19 Jan. 2014, <https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf>.

Perera, G 2012, *Purposefully manufactured vulnerabilities in US government technology microchips: risks and homeland security implications*. Ph.D. Naval Postgraduate School.

Pfleeger, CP 1997 'The fundamentals of information security', *Software*, IEEE, vol. 14, no. 1, pp. 15-16.

PwC 2013a, *PricewaterhouseCoopers: China's impact on the semiconductor industry 2013 update,* viewed 11 Jan. 2014, <http://www.pwc.com/gx/en/technology/chinas-impact-on- semiconductor-industry/assets/china-semicon-2013.pdf>.

— 2013b, *PricewaterhouseCoopers: The Global State of Information Security® Survey 2014*, viewed 2 Jan. 2014, <http://www.pwc.com/gx/en/consulting-services/information-security- survey/download.jhtml>.

Rainer, RK, Marshall, TE, Knapp, KJ, & Montgomery, GH 2007 'Do information security professionals and business managers view information security issues differently?', *Information Systems Security*, vol. 16, no. 2, pp. 100-108.

Reuters 2013, *Exclusive: Secret contract tied NSA and security industry pioneer*, viewed 11 January 2014, <http://www.reuters.com/article/2013/12/20/us-usa-security-rsa- idUSBRE9BJ1C220131220>.

Schroeder, NJ & Grimaila, MR 2006 'Revealing prospect theory bias in information security decision making', *Emerging Trends and Challenges in Information Technology Management: 2006 Information Resources Management Association International Conference*, ed. M Khosrow-Pour, pp. 176-179.

Shostack, A & Stewart, A 2008, *The New School of Information Security*. Addison-Wesley, Boston.

Skorobogatov, S & Woods, C 2012 ‘Breakthrough silicon scanning discovers backdoor in military chip’, *Proceedings of the 14th international conference on Cryptographic Hardware and Embedded Systems*, eds. E Prouff & P Schaumont, pp.23–40.

SST 2012, *Solid State Technology: Top 12 semiconductor foundries of 2012*, viewed 11 Jan. 2014, <http://electroiq.com/blog/2012/08/top-12-semiconductor-foundries-of-2012/>.

Tarnovsky, C 2008, *Black hat DC - February 21, 2008 presentation: Security failures in secure devices*, viewed 28 Jan. 2014, <http://www.blackhat.com/presentations/bh-dc-08/Tarnovsky/Presentation/bh-dc-08-tarnovsky.pdf>.

Tsiakis, T & Stephanides, G 2005 ‘The economic approach of information security’, *Computers & Security*, vol. 24, no. 2, pp.105–108.